Call Houston

GDPR Whitepaper

Prepare for privacy:

“The fundamental right to privacy”

GDPR whitepaper: Prepare for privacy

Call Houston

Content

- Introduction Page 3
- To whom does this apply? Page 4
- Impact on daily business Page 5
- New processes to adopt Page 6
- Approach and checklist Page 7
- GDPR and Shopify Page 8
- GDPR and VendHQ Page 9
- Additional Page 10

”The GDPR makes individuals owners of their data. It is the most ambitious data protection legislation ever passed and is setting a new global standard for privacy and data security”

Introduction

Call Houston

- The General Data Protection Regulation (GDPR) is the latest privacy act from the European Union (EU) which impacts all businesses who collects, stores, uses and/or processes data on individuals resident in the EU.
- The EU has since the second world war had a deep belief in personal privacy. The first global example of this was the 1995 Data Protection Directive (DPD), demanding governments and companies to be transparent about what data they keep, to have legitimate reasons to keep the data and to handle the data with care.
- The GDPR is an update to the DPD due to the vast increase in data that businesses keep and collect and to have the legislation relevant for the world of today. It grants extensive privacy rights to individuals and places a large obligation to companies to ensure that the right processes are followed and that data is handled in an appropriate manner. It also extends the liability of companies, passing on data to third parties.
- The GDPR follows a range of scandals of leaks and unappropriated processes of personal data protection, most significantly the Facebook and Cambridge Analytics data protection scandal.
- This whitepaper outlines the consequences of the GDPR for merchants selling online. It further provides a guiding approach on how to best adopt the new legislation throughout the organization.

To whom does this apply?

Call Houston

Application

- The GDPR applies to any business who collects, stores, uses and/or processes data on individuals resident in the EU.
- The GDPR is specifically aimed at “personal data”, meaning any data that refers to an individual (data subject). Particularly information regarding:
  - Name
  - Identification number
  - Location data (address)
  - Online identifier (IP addresses or cookies)

Controller

- The entity who obtains and controls for what purposes and how personal data is processed
- In general this is the **merchant**
- In case a 3rd party is involved in the purchasing process on request of the merchant, it is the responsibility of the merchant to make sure the party conforms to the GDPR legislation policy

Processor

- The entity who processes the data on behalf of the controller
- In general this is the **platform** hosting a system or website. e.g. Shopify, VendHQ, Google.
  - The processor may only process data upon pre-authorization from the controller.
  - Processor must document and erase data upon request (DPIAs)

Data flow scenarios when individual visits and/or purchases from a store

1	Buyer (data subject)	Merchant (controller)	Platform (processor)	
2	Buyer (data subject)	3rd party (controller)	Merchant (processor)	Platform (sub-processor)
3	Buyer (data subject)	Merchant (controller)	Platform (processor)	3rd party (sub-processor)

Impact on daily business

Call Houston

Customer rights

- Under the GDPR legislation, data subjects can request the following from the data controller:
  - Data erasure
  - Data correction
  - Data access
  - Data export in a common and portable format
- The controller must accordingly follow this request through to 3rd parties and processors possessing this particular information

Personal data transparency obligations

Facilitating requests

- Merchants are obliged to help data subjects exercise their rights under GDPR

Complying with marketing and cookie regulation

- Merchants must obtain consent when collecting and/or using cookies from the data subjects

Posting visible privacy notice

- Merchants must inform data subjects about the data collected and how to access it

Children's data processing

- Merchants must obtain consent from parents when obtaining data from children below 16yrs of age

New processes to adopt

Call Houston

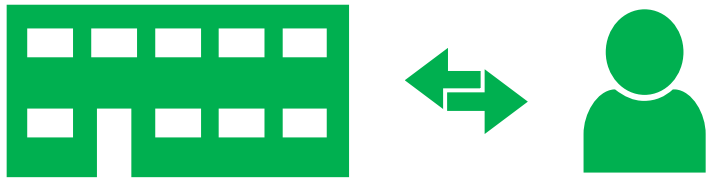
Authorizing requests

- Upon request, merchants must provide action within 30 days of the request, unless the request is highly complicated
- Before processing a request from a data subject, merchants must authorize that the request is coming from the data subject and that there is no legal reason to preserve the data
  - Authorization of the applicant to present an image with the data subject and valid ID card

3rd party validation

Merchants are required to make sure 3rd party integrations live up to and know how to process data requests

Facilitating requests



Data erasure

- Merchants are obliged to help data subjects erase their data from both the controller and the processor
- Clear and visible processes must be in place on how to facilitate this

Data correction

- Data subjects have the right to request a change in their data to reflect reality
- Clear and visible processes must be in place on how to facilitate this

Data access

- Data subjects must have access to the data which is being held by the controller or processor
- Clear and visible processes must be in place on how to facilitate this

Data export

- Merchants must have the ability to export data in a common format (e.g. csv) to hand over to data subjects
- Clear and visible processes must be in place on how to facilitate this

Approach and checklist

Call Houston

1. Raise awareness in your organization

- A great deal of the GDPR is changing the mindset of the confidentiality of personal data and how the organization stores and processes this

2. Implement processes to facilitate requests

- Clear processes on how to facilitate data requests is an essential start on how to comply with the GDPR
- Further, to make as much information easy accessible and editable for data subjects as possible

3. Communicate compliance with GDPR

- Communicate to existing customers on how and where to exercise their rights under GDPR
- Implement information for live data gathering for future visitors and customers

4. Check suppliers and 3rd part integrations

- Follow up on processor, sub-processors, 3rd party integrations and other entities with whom the business is sharing data, that they are complying with GDPR
- Set processes for requests to 3rd parties

External

- ❑ Communicate cookie policy online to visitors
- ❑ Update privacy policy in conformity with GDPR when people check out
- ❑ Communicate conformity with GDPR and how customers can exercise their rights
- ❑ Confirm “data policy confirmation step” in purchases

Internal

- ❑ Raise awareness of the seriousness of the legislation change
- ❑ Update and inform of internal processes
- ❑ Set action plan in case of breach of date security or leakage
- ❑ Clear conformity to GDPR with 3rd party suppliers and integrations
- ❑ Facilitate for customers to edit their own information online via customer login
- ❑ Redefine what information is collected and why this is collected

Organizational measures

- ❑ Update who has access to customer data
- ❑ Set role restrictions on who can see what (e.g. for Shopify and VendHQ)
- ❑ Enable two-factor authentication
- ❑ Regularly overview activity logs
- ❑ Appoint data security officer (if applicable)

GDPR and shopify

Call Houston

- Shopify acts as processor in that they provide a platform for merchants
- In General, Shopify has taken wide measures to comply with the GDPR legislation across both data streams, storing, processing and facilitating personal data requests.
- Shopify will upon request and pre-authentication, erase some or all data on a data subject. This includes all data that related to the individual, however, Shopify reserves the right to anonymize other information as sales figures, SKUs, etc.
- Shopify has a strong cross-functional data protection program which ensures the security of data subjects personal data and the conformity with the GDPR legislation.
- Shopify has obtained following certifications for data processing security standards: Tier III, ISO 27001, PCI-DSS, additionally all Shopify hosted stores are Level 1 PCI-DSS secured
- Shopify has incorporated the data processing agreement with data controllers in their terms and conditions for Shopify plans.
- Further information about Shopify transparency and data handling will be published at the end of 2018

General points

- Shopify data request facilitation is to be forwarded to: privacy@shopify.com
- Hosting your store with Shopify does not make you automatically comply with GDPR, internal processes and initiatives must also be taken as the merchants role of controller

GDPR and vend

Call Houston

- VendHQ acts as processor in that they provide a platform for merchants
- In General, VendHQ is taking wide measures on complying with GDPR and more is still at this point being prepared. Vendhq still do not have the option to fully delete or to scrutinize data requests. This will be updated by Vend soon.
- You can in your Vend dashboard erase some or all data on a data subject. This includes all data that related to the individual, however, VendHQ reserves the right to anonymize other information as sales figures, SKUs, etc.
- VendHQ have been updating the terms of use and privacy policy to make sure VendHQ merchants are complying with the GDPR legislation.

General points

- Vend merchants must sign a DPA agreement with VendHQ. Sign
- Using VendHQ eCommerce or POS does not automatically make your business comply with the GDPR, as the role of controller you must still comply with the controller obligations

Additional

Call Houston

Key considerations in GDPR regards

Base of data processing

- In order to process personal data, organizations must have a lawful basis to process the data, that consent must be freely given, specific, informed, and unambiguous. In other words, organizations must give data subjects a genuine choice whether to allow their data to be processed, and data subjects must agree via a clear statement or affirmative action. Additionally, organizations must be able to prove that they obtained valid consent.

Compliance obligation

- The GDPR places numerous direct compliance obligations on data processors. This includes requirements that processors only process personal data in accordance with the controller's instructions, not share data with other vendors without consent of the controller, and implement appropriate security.

Breach notification

- Data controllers must report any data breach to their data protection authority as soon as possible and no later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in any harm to the data subjects. If there is a high risk of harm, data controllers must report data breaches to the data subjects as soon as possible. Data processors must also notify data controllers of data breaches as soon as possible.

Direct link to the GDPR regulation

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Call Houston is dedicated in supporting the compliance and successfully implementation of GDPR to its partners. This Whitepaper provides for a better understanding and approach on how companies can comply with the new legislation. This whitepaper is to serve as a guiding line, not as a lawfully checklist to defend the compliance with GDPR. For further legislative compliance, we recommend consulting a data security lawyer.